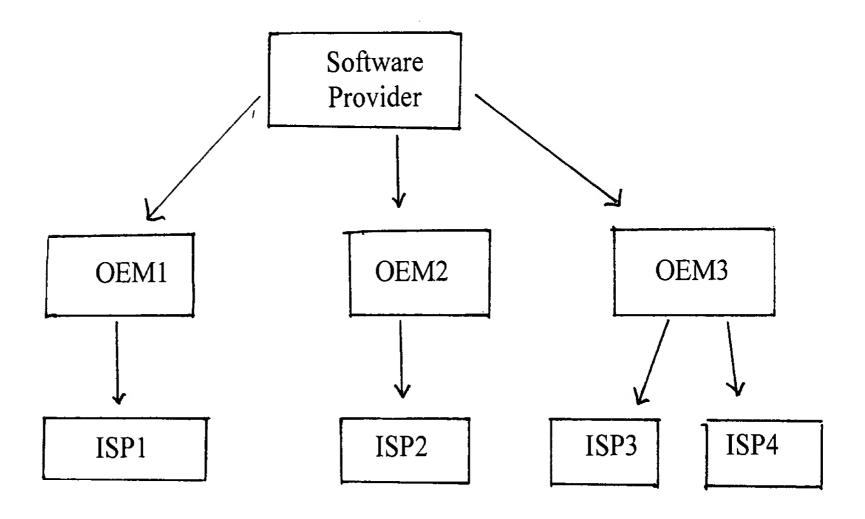


FIGURE 1

Sample Business Hierarchy



=4

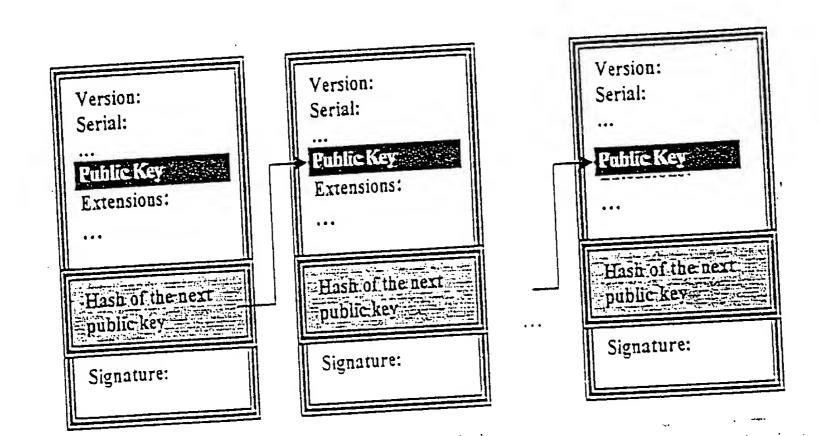
Gur Tark Tre

France Z.

General Format of X509 Version 3 Certificate

Version
Serial Number
Algorithm Identifier
Issuer
Period of Validity
Subject Name
Subject Public Key
Extensions
Signature

-06-



F16.3 Root Certificate Chaining



SAMPLE OEM RSIO

OEM Root Certificate

(note: For an SP RSIO the entire chain of SP Root Certificates would be included. For an ISP RSIO the ISP Root Certificate would be included.)

(Trusted Entity's Identity)	(Trust Information)	(Delegation Information)
Entity 1 Fingerprint	Entity_1 trust information	Entity_1 delegation information
Entity_2 Fingerprint	Entity_2 trust information	Entity_2 delegation information
•••	•••	•••
Entity m Fingerprint	Entity_m trust information	Entity_m delegation information
CA_1 Fingerprint	CA_1 trust information	CA_1 delegation information
CA_2 Fingerprint	CA_2 trust information	CA_2 delegation information
•••		•••
CA_n	CA_n trust information	CA_n delgation information
	Timestamp	
	Signature	

FIG. 5 SAMPLE TRUST-DELEGATION VECTOR

BIT	DESCRIPTION
0	CA trusted to issue certificates for SSL clients
1	CA trusted to issue certificates for SSL servers
2	CA trusted to issue certificates for SP clients
3	CA trusted to issue certificates for SP servers
4	CA trusted to issue certificates for SP system software publishers
5	CA trusted to issue certificates for SP application software publishers
6	CA trusted to issue certificates for step-up encryption servers
7	Entity trusted as OEM, can issue OEM RSIOs
8	Entity trusted as SP, can issue SP RSIOs
9	SP server instance
10	SP system software publisher
11	Application software publisher

FIG. 6 Schematic of Hierarchical Security Information Object

=£

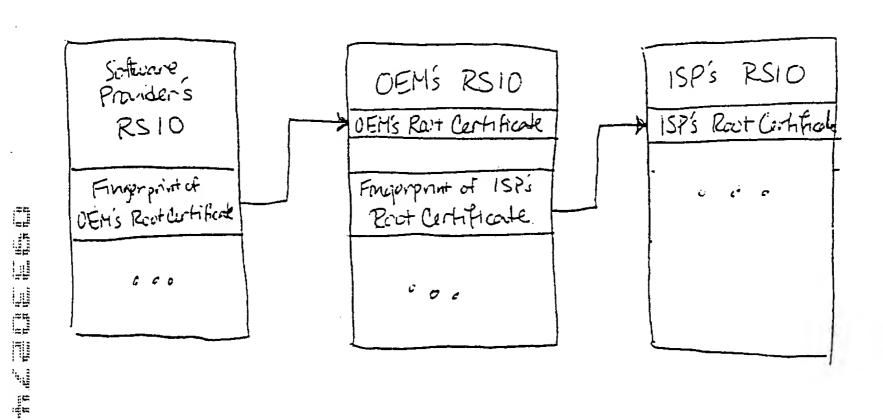
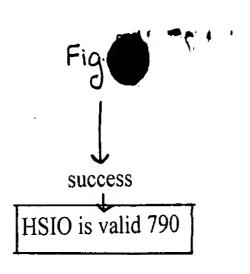


FIG. 7A Validation of an HSIO by ISP client Receive an HSIO from ISP 710 HSIO is invalid 725 Check that the ISP's Root Certificate in the HSIO is not expired expired 720 not expired Validate the ISP's RSIO (by verifying its signature HSIO is invalid 735 fails using the ISP's root certificate included in the RSIO) 730 Success HSIO is invalid 745 Validate that the ISP's root certificate is fails contained in the OEM's RSIO 740 Success HSIO is invalid 755 Check that the OEM's root certificate is not expired 750 expired į: · not expired == HSIO is invalid 765 Validate the OEM's RSIO (by verifying its signature fails using the OEM's root certificate in the OEM's RSIO) 760 Success Validate that the OEM's root certificate is fails HSIO is invalid 775 included in the ISP's RSIO 770 Success Validate the SP's RSIO -- by chaining from the most HSIO is invalid 785 fail recent root certificate in the RSIO backwards to the latest locally known valid root certificate, as discussed in the Detailed Description and disclosed in the Incorporated Disclosures 780



NCI-061 Fig. 7B

• :



FIG. 8
Authentication of an SSL server certificate from non-partner SSL server

